(2)

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DEFENSE DATA NETWORK AND THE
NAVAL SECURITY GROUP

by

Jean M. Eberhardt

March 1988

Thesis Advisor: Norman F. Schneidewind
Co-Advisor: Judith H. Lind

Approved for public release; distribution is unlimited

Unclassified

security classification of this page

REPORT DOCUMENTATION PAGE

1a Report Security Classification Unclassified	1b Restrictive Markings
2a Security Classification Authority	3 Distribution Availability of Report Approved for public release; distribution is unlimited.
2b Declassification Downgrading Schedule	
4 Performing Organization Report Number(s)	5 Monitoring Organization Report Number(s)
6a Name of Performing Organization Naval Postgraduate School	6b Office Symbol *(if applicable)* 62
7a Name of Monitoring Organization Naval Postgraduate School	
6c Address *(city, state, and ZIP code)* Monterey, CA 93943-5000	7b Address *(city, state, and ZIP code)* Monterey, CA 93943-5000
8a Name of Funding Sponsoring Organization	8b Office Symbol *(if applicable)*
9 Procurement Instrument Identification Number	
8c Address *(city, state, and ZIP code)*	10 Source of Funding Numbers

Program Element No	Project No	Task No	Work Unit Accession No

11 Title *(Include security classification)* DEFENSE DATA NETWORK AND THE NAVAL SECURITY GROUP

12 Personal Author(s) Jean M. Eberhardt

13a Type of Report Master's Thesis	13b Time Covered From To	14 Date of Report *(year, month, day)* March 1988	15 Page Count 60

16 Supplementary Notation The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

17 Cosati Codes

Field	Group	Subgroup

18 Subject Terms *(continue on reverse if necessary and identify by block number)*
Defense Data Network, Naval Security Group, DDN, NSG.

19 Abstract *(continue on reverse if necessary and identify by block number)*

This thesis describes the Defense Data Network (DDN) and its possible applications for the Naval Security Group. It reviews the background and historical information that contributed to the selection of DDN as the primary long distance data communications system for the Department of Defense. It evaluates some of the advantages and disadvantages of packet switching technology. The survivability, availability, and security features of DDN are presented. Also included are specifications of the hardware equipment, software standards, and operating procedures for DDN. The Naval Security Group does not require direct DDN access to accomplish its operational mission. There are, however, a number of nonoperational requirements that could be facilitated by direct DDN access. This thesis discusses a potential role for DDN in the Naval Security Group. Applications for administration, personnel, supply, and logistics functions are provided. Uses for the electronic mail, remote access, and file transfer networking functions of DDN are also proposed. Potential benefits resulting from DDN access are presented along with recommendations for further investigation.

[illegible] S. NSG

20 Distribution Availability of Abstract ☒ unclassified unlimited □ same as report □ DTIC users	21 Abstract Security Classification Unclassified
22a Name of Responsible Individual Norman F. Schneidewind	22b Telephone *(include Area code)* (408) 646-2768
22c Office Symbol 54Ss	

83 APR edition may be used until exhausted
All other editions are obsolete

security classification of this page

Unclassified

Defense Data Network
and the
Naval Security Group

by

Jean M. Eberhardt
Lieutenant, United States Navy
B.S., United States Naval Academy, 1983

Submitted in partial fulfillment of the
requirements for the degree of

MASTER OF SCIENCE IN TELECOMMUNICATIONS SYSTEMS
MANAGEMENT

from the

NAVAL POSTGRADUATE SCHOOL
March 1988

Author: Jean M. Eberhardt
Jean M. Eberhardt

Approved by: Norman F. Schneidewind
Norman F. Schneidewind, Thesis Advisor

Judith H. Lind
Judith H. Lind, Co-Advisor

David R. Whipple, Chairman,
Department of Administrative Science

James M. Fremgen,
Acting Dean of Information and Policy Sciences

ABSTRACT

This thesis describes the Defense Data Network (DDN) and its possible applications for the Naval Security Group. It reviews the background and historical information that contributed to the selection of DDN as the primary long distance data communications system for the Department of Defense. It evaluates some of the advantages and disadvantages of packet switching technology. The survivability, availability, and security features of DDN are presented. Also included are specifications of the hardware equipment, software standards, and operating procedures for DDN. The Naval Security Group does not require direct DDN access to accomplish its operational mission. There are, however, a number of nonoperaticnal requirements that could be facilitated by direct DDN access. This thesis discusses a potential role for DDN in the Naval Security Group. Applications for administration, personnel, supply, and logistics functions are provided. Uses for the electronic mail, remote access, and file transfer networking functions of DDN are also proposed. Potential benefits resulting from DDN access are presented along with recommendations for further investigation.

TABLE OF CONTENTS

LIST OF FIGURES

I. INTRODUCTION

A. DEFENSE DATA NETWORK

The United States Department of Defense (DoD) communications system is in a period of transition from its aging Automatic Digital Information Network (AUTODIN) to the new Defense Data Network (DDN). This transition involves record message traffic and data communications processed by most DoD Agencies. In order to use available resources effectively, a replacement project of such large magnitude requires much planning by program managers as well as prospective users. The purpose of this thesis is to investigate possible applications of DDN for the U.S. Naval Security Group Command; the intended audience is Navy managers and planners associated with the Security Group. Readers affiliated with other organizations also may obtain relevant information concerning transitions to DDN. The sources from which this information has been compiled include: published articles on various aspects of DDN, briefings presented at the 1987 Navy DDN Program Management Review, and interviews with Naval Security Group managers representing Security Group headquarters and field stations.

DDN is a replacement for AUTODIN, but it is also a great deal more. It uses a revolutionary new type of switching technology, called packet switching, and has modern networking capabilities which are not available on AUTODIN. These enhanced network functions include electronic mail, the ability to send notes between individual users; telnet, the ability to access information at a remote location; and file transfer protocol, the ability to transfer complete stored files from one network user to another. It is the availability of these new functions which prompts this research into direct accession to DDN by the Naval Security Group.

B. NAVAL SECURITY GROUP

Naval Security Group, the cryptologic element of the U.S. Navy, supports Fleet Staffs and operates commands, departments, and detachments worldwide in various types of facilities. There is presently no plan for these entities to gain direct access to DDN and this access is not necessary for the Security Group's operational mission. But in light of DDN's advanced capabilities and the fact that most other Navy commands may soon be capitalizing on electronic mail and the other new network functions, it is worthwhile to view DDN as a potential resource on an administrative basis. This study makes recommendations concerning the feasibility and appropriateness of connectivity to DDN by Naval Security Group organizations.

C. GOALS AND OBJECTIVES

The goals of this thesis are

1. To introduce DDN and its features to Naval Security Group personnel.
2. To identify possible DDN applications for Naval Security Group elements.
3. To provide Naval Security Group managers with enough information to consider DDN access for their commands.

II. BACKGROUND

This chapter contains the background information that forms the foundation of this research. The first section discusses current trends towards the integra'ion of computer and communication networks; it is presented so that this thesis will be relevant to planners involved with human-to-human and human-to-computer, as well as computer-to-computer applications. A short history and explanation of the technology of the DDN is included in the second section in order to provide a basis for future discussion of its strengths and weaknesses. Finally, the various components of the Naval Security Group Command are introduced.

A. NETWORKING

The term network is defined by Stoner as the linking of groups of computers, either within an organization or between multiple organizations, so that they can communicate with each other and share common data bases and resources [Ref. 1: p. 693]. That author also uses the term networking to represent an individual's sphere of influence, both received and dispersed. In the context of this study, it is worthwhile to consider networking as both a hardware and an interpersonal resource. Being able to share common data bases and broaden a network of associates enhances the likelihood of a member of any organization fulfilling the premise that "...it is both what you know and who you know that counts" [Ref. 1: p. 553]. DDN offers many networking functions, but it is important first to realize current applications of networks in general so that the study of specific choices involving DDN options can be made in proper perspective.

Networks can be configured to connect individuals within an organization or to link separate organizations together. User-oriented networks within a centralized organization are commonly referred to as local area networks. Long-distance, or long-haul, networks are usually public utilities for many organizations and can sometimes even provide worldwide services. The local area network configuration is rapidly replacing the direct access of individual terminals to the DDN.

This integration of local area considerations into the overall scheme of long-haul networks has emphasized the need for interoperability between networks. The merger of the fields of computer science and data communications, which occurred during the 1970s and 1980s, also has emphasized the need for interoperability among managers of each discipline. The merger is discussed by Stallings who states that the computer-communications revolution has occurred and has pr duced the following results:

- There is no fundamental difference between data processing (computers) and data communications (transmission and switching equipment).
- There are no fundamental differences among data, voice, and video communications.
- The lines between single-processor computer, multiprocessor computer, local network, metropolitan network, and long-haul network have blurred. [Ref. 2: p. 1]

Accepting these assumptions, this paper proceeds to analyze DDN as an integrated communications system that is easily accessible to different forms of data and information. In fact, long-range planners within the Defense Department foresee the DDN evolving with the new Defense Switched Network to form a fully integrated data and voice network [Ref. 3: p. 35.1.1].

B. DEFENSE DATA NETWORK

DoD communications managers should become acquainted with the evolution and mechanics of the DDN, since it will eventually provide connectivity for all DoD entities. Familiarization with past and projected network structures as well as with the DDN technology will assist individual managers in making wise decisions during the establishment of smooth transition plans for each DoD organization.

DDN is not only of interest to DoD communications managers but is also important to computer system managers. Investigation into the evolution of DDN reveals that efficient use of computer facilities and interoperability between subscriber resources were high priorities during the developmental stages of DDN [Ref. 4: p. 15.5.1]. The DDN historical and technological information presented here should prove useful to both communication and computer systems managers.

1. History

The Defense Advanced Research Projects Agency initiated a packet switched network in 1969 as an intra-agency communications system and as an experiment investigating new technologies. Members of this research community, mindful of the need to share information and aware of the benefits of accessible databases, desired to employ true networking functions on a cross-continental basis. Networking functions (such as office automation and file transfers) had previously been employed only in local area networks consisting of similar types of computers. But the research agency's network, known as ARPANET, proved that users of different types of computers could share programs and communicate over long distances [Ref. 5: p. 8].

ARPANET grew rapidly, allowed participation outside the agency, and gained acceptance by many operational users. As a result of this success, in 1975 the Defense Communications Agency (DCA) assumed responsibility for the network. Throughout this time period (1969-1980) DCA also developed plans for a replacement AUTODIN II system which would use packet switching technology. In 1981, DCA initiated a study comparing the planned AUTODIN II to ARPANET. It was no longer beneficial to support the development of two packet-switched networks, so, based on risk, cost, and expandability, the study ruled in favor of ARPANET's proven technology over the AUTODIN II plans. The DDN project was started and AUTODIN II was canceled in April 1982.

The core of DDN was the existing ARPANET, and its war and peacetime mission is to provide the DoD reliable, survivable, and secure worldwide communications service and the ability to transmit according to precedence requirements [Ref. 6: pp. 59-60]. Building on an existing network enabled DDN project managers to realize an early availability date and to benefit from some on-line experience. However, use of ARPANET also prevented some ground-zero decisions concerning standard network protocols and necessitated the inclusion of equipment that was already becoming obsolete.

The future DDN does not depend on the early success of ARPANET, but instead relies on continued evolution and incorporation of today's ever-improving hardware and software technologies. Hurlburt cites the overwhelming effect of too many software options in particular as the downfall of AUTODIN II [Ref. 7: p. 62]. DCA now has the challenge of keeping all branches of DDN standardized while continuing to offer innovations to users.

The commitment to DDN by the Office of the Secretary of Defense was declared in a memorandum to the Secretaries of the Military Departments dated March 10, 1983. The memorandum states:

> All DoD automatic data processing systems and data networks requiring data communication services will be provided long haul and area communications, interconnectivity, and the capability for interoperability by the DDN. Existing systems, systems being expanded and upgraded, and new automatic data processing systems or data networks will become DDN subscribers. [Ref. 8: p. 1]

Present guidance from the Office of the Secretary of Defense is still consistent with this memorandum. DoD communities are just beginning to connect to DDN. As the network continues to expand, more DoD personnel will become DDN users (subscribers).

When the DDN project was initiated in response to the Secretary of Defense Memorandum, the research segment of the network retained the name ARPANET, and the operational user network was designated as the Military Network (MILNET). There are now other segments of DDN and each one continues to expand. Some examples of DDN segments include the Strategic Air Command Digital Network, Worldwide Military Command and Control System Intercomputer Network Communications Subsystem, and the DoD Intelligence Information System. These DoD communities established their own networks in order to contain classified information to a limited environment. They are physically separate networks, managed by DCA, but not yet consolidated into a true DoD network. Gateway devices currently under development will eventually allow internetworking between communities. Figure 1 on page 7 shows an internetwork environment.

The physical structure of DDN consists of backbone and access networks. The backbone refers to the centralized core of DDN that allows data to travel long distances. It consists of relay stations (packet switching nodes) connected by terrestrial or satellite communications links (interswitch trunks). The users' terminals, computers, and connecting circuits comprise the DDN access components. Figure 2 on page 8 illustrates the backbone and access framework.

The DDN segments handling information at various levels of classification presently have physically separate backbones. However, the planned incorporation in 1988 of end-to-end encryption equipment, known as Blacker devices, will enable information from a sensitive network to traverse the same interswitch trunk as does information from the unclassified MILNET segment [Ref. 6: p. 60].

The classification of DDN into its various community-of-interest segments and into its hardware configurations highlights the challenges facing project management in the area of interoperability. True DDN interoperability would mean that a user from any DoD community could use DDN resources to communicate with a user from any other DoD entity. As program manager, DCA provides the node computers and leases appropriate telephone lines for communication among backbone components. DCA must also ensure interoperability among the various military service subscribers who

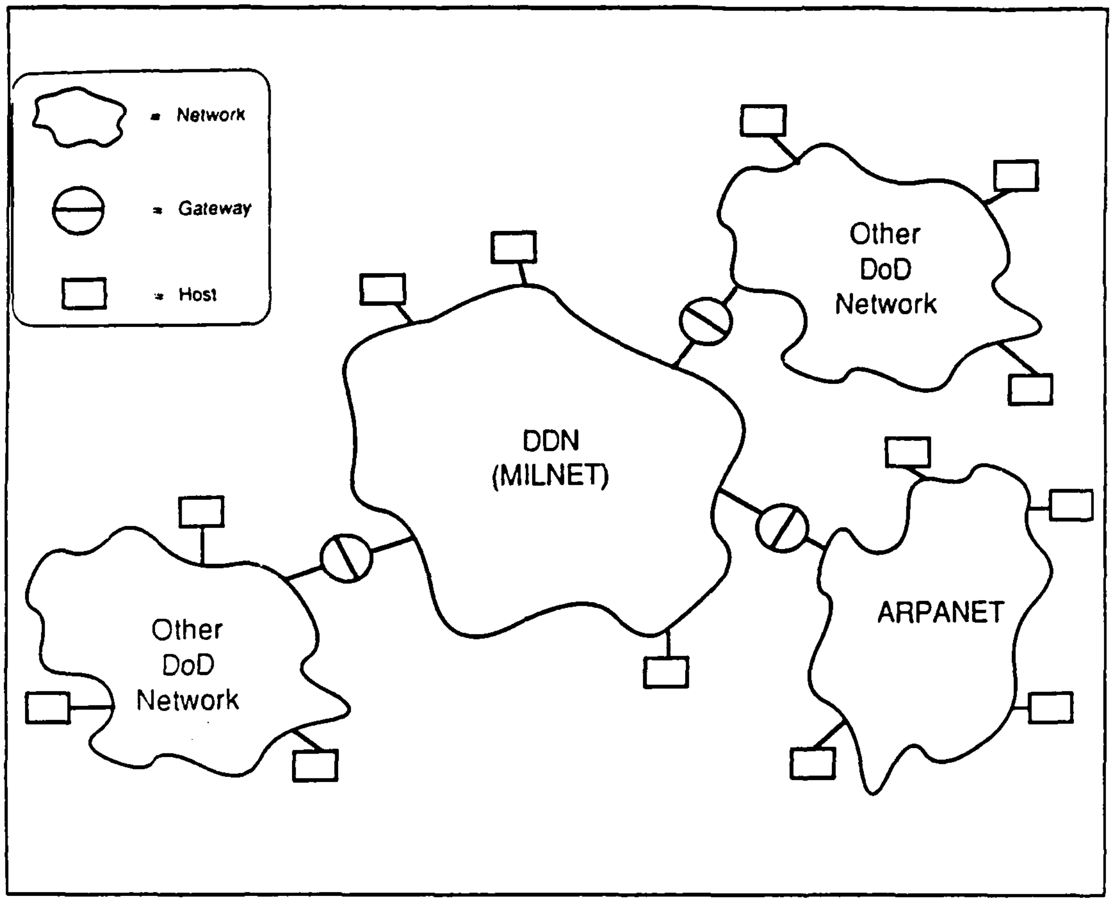

Figure 1. DoD Internetworking Environment. [Ref. 9: p. 4-10a].

provide their own terminals, modems, and host computers to access DDN [Ref. 5: p. 9].

2. Technology

Communications systems provide paths to relay information between users. Today's transmission paths travel through cables, microwave antennas, and satellites. Networks conserve these resources by using one transmission path to connect many users. The process of changing a given path from one point-to-point link to another is known as switching.

Three common forms of switching techniques are circuit switching, message switching, and packet switching. Circuit switching involves the actual physical switching of network resources while message and packet switching refer to the selection of a route over available resources. ARPANET pioneered packet switching technology, and DDN

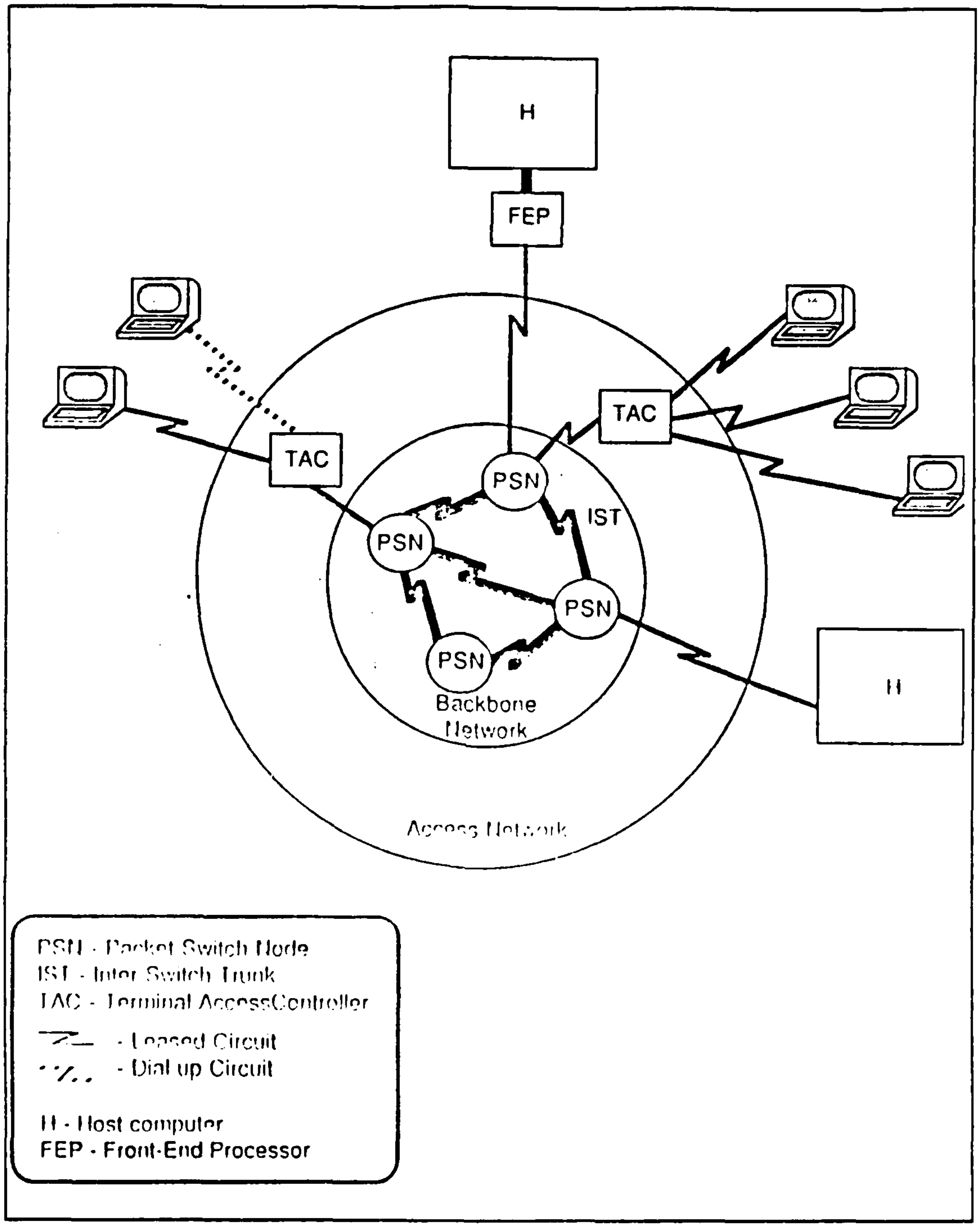

Figure 2. DDN Backbone and Access Structure. [Ref. 9 p 5-4a]

continues to capitalize on this extremely efficient method. A useful way to describe packet switching is to compare it to existing systems.

The most familiar communications system is the DoD telephone network, called Automatic Voice Network (AUTOVON), that uses circuit switching technology. Each time a call is placed, switching centers connect a circuit between the sender and receiver. This provides a dedicated link that is well suited to interactive voice conversations. The conversations will not be interrupted unless precedence requirements warrant. Then the AUTOVON system may switch circuit resources from a routine call to one of higher priority. Circuit switching is not very efficient because only two users exploit the available transmission equipment and bandwidth of any path at any given time. [Ref. 9: pp. 2-1,2-2]

The AUTODIN system uses message switching technology. Each message is entered into the system as a unit and travels an established route from its source to the nearest AUTODIN switching center. The 15 AUTODIN switching centers located worldwide act as hubs to direct messages to the switching center nearest to the intended message destination. Message switching allows the paths between switching centers to serve many users simultaneously. This is more efficient than circuit switching but does not allow users to interact on a timely basis. [Ref. 9: pp. 2-3,2-4] DDN's packet switching technology makes message switching even more efficient by dividing messages into smaller packets that are routed individually.

In addition to routing information as smaller segments, DDN also has a more distributed structure than AUTODIN. DDN consists of hundreds of switching nodes that can process the packets, while AUTODIN has only 15 switching centers to accomplish its message switching routines. DDN packet route selections are dynamic; each packet travels the most expeditious route at any given time.

In terms of time savings, the packet transits can be compared to people driving their own cars instead of waiting to travel together on a bus. Messages that currently stack up in queue at AUTODIN switching centers will bypass busy or inoperative packet switching nodes and speed along to their destinations on the DDN system. A limited number of roads and use of a separate car for each person can cause vehicular traffic jams; similarly, an efficient transportation system for information must have sufficient capacity and a reasonable amount of data included in each packet.

The ability of DDN's routing algorithm to adapt to changing network configurations contributes to its survivability, reliability, and flexibility. The fact that each interswitch trunk passes interleaved bits of many messages instead of complete communications or data transfers enhances the security aspect of the DDN. These attributes were the basis for the selection of DDN as a major telecommunications resource for DoD. As DDN gains acceptance throughout the military services, organizations such as the Naval Security Group should carefully consider what DDN has to offer.

C. NAVAL SECURITY GROUP

Background information presented in this section serves two purposes. First, it provides an introduction for readers who may not be familiar with the Naval Security Group Command. Second, it should help readers who are associated with the Security Group consider this thesis in the context of the Naval Security Group as an entire organization, not on the basis of the reader's viewpoint which may be limited to that of an administrator, communicator, engineer, or operator.

Naval activities that report to the Commander of the Naval Security Group vary in size and are located throughout the world. An understanding of the structure of the Naval Security Group is necessary in order to evaluate proposals related to networking on a naval base level, at a type commander level (such as Commander, Naval Security Group), or on a Navy-wide level.

1. Organization

The Offices of the Secretary of Defense are responsible for ensuring interoperability among services and overall support of national interests, while the individual military departments use their allotted manpower and equipment to accomplish specific missions. DCA is DoD's vehicle for overall management of the Defense Communication System, and the Naval Telecommunications Command is the Navy's long-haul communications authority. The Commander, Naval Telecommunications Command, reports directly to the Chief of Naval Operations for configuration control of the Naval Telecommunications System, and is the Navy's program manager for the DDN project.

The Commander of the Naval Security Group (COMNAVSECGRU), like the Commander of the Naval Telecommunications Command, is a second echelon commander reporting directly to the Chief of Naval Operations. The Security Group consists of commands of various sizes and at various locations. Some of the commands are independent naval bases and others are tenants of naval or air force bases or army posts. If applicable, a Naval Security Group Activity (NSGA) commanding officer may report to a base commanding officer or commander on matters relating to base administration and to the local area coordinator for regional naval policy. Fleet commanders may levy operational tasking on NSGA sites, but COMNAVSECGRU is the administrative manager responsible for ensuring the proper functioning of NSGAs.

COMNAVSECGRU has authority over NSGAs that are located throughout the world. In addition to the field activities commanded by its own officers, the Naval Security Group also mans a department in most of the navy communications stations and communications area master stations. There are also Naval Security Group personnel stationed at detachments remotely situated from parent commands and members assigned to staff duty. Staff assignments could be to the COMNAVSECGRU Headquarters staff in Washington, D.C., or to a number of other fleet staffs that require cryptologic expertise.

Officers and enlisted personnel whose duties directly contribute to the Naval Security Group operational mission are assigned appropriate designators or ratings that identify them as cryptologic officers or technicians. This means that for the majority of their careers these people will serve in billets under the purview of COMNAVSECGRU. Navy personnel whose duties are in support of Naval Security Group facilities, such as civil engineers and supply officers, are not permanently associated with COMNAVSECGRU and usually serve only one tour in a Security Group capacity. Within the Naval Security Group, manpower resources are divided into various branches that identify areas of expertise, such as maintenance, administration, or communications.

2. NAVSECGRU Communication

COMNAVSECGRU headquarters and field activities are divided by functions that are organized in hierarchies similar to traditional naval shipboard organizations. Depending on the size of the NSGA, its divisions and departments are arranged according to functions such as operations, electronic maintenance, facilities maintenance, administration, training, and communications. As previously described, the communications systems of DoD and the Department of the Navy are upgrading to packet-switched networks; the Security Group is no exception. All DoD cryptologic elements will eventually participate in a packet-switched network for their special community of interest under a project known as Platform [Ref. 10]. Just as the cryptologic community's special communications system interfaces with the general service navy at AUTODIN switching centers today, the future system will interface with DDN via interservice/agency automated message processing exchanges.

The Naval Security Group presently maintains its own communications equipment that is compatible with the rest of the navy and DoD only through the interfaces of AUTODIN switching centers. To date, these interfaces have been sufficient for interorganizational communications. However, the advent of enhanced networking functions (that will not be immediately available through automated message processing exchanges) raises the possibility of direct access to MILNET by Naval Security Group entities.

III. DDN FEATURES

Plans for DDN include expansion to a worldwide network. This requires every aspect of DDN to be flexible towards additions and adjustments. Several noteworthy DDN features have contributed to its initial success and will greatly enhance future expansions. Three features contributing to the overall effectiveness and flexibility of DDN are its survivability, availability, and security.

A. SURVIVABILITY

One outstanding attribute of DDN is its projected ability to continue to function during a crisis. No system is invulnerable, but the goal of DDN is to continue to provide vital DoD communications after a disaster has occurred. Both natural and enemy inflicted disasters can damage DDN. The natural types (earthquakes and devastating storms) normally affect a limited geographic region that may not include many DDN resources. The other types (conventional or nuclear attacks) more likely would affect DDN since military installations would be probable targets.

Indications and warnings may precede full scale enemy attacks, but DDN planners must also guard against the unpredictable possibilities of natural disasters and terrorist sabotage. Individual users of DDN protect their communications equipment with the same physical security measures that safeguard the rest of their base or post facilities. The packet switching nodes of the shared backbone of DDN also benefit from military installation protection because often the nodes are colocated with one of the subscribers.

Fences, sentries, and locked buildings are among the physical security measures that protect DDN from threats against specific locations. The distributed nature of the network as a whole contributes to its overall survivability. The loss of any portion of DDN should not affect the operation of the remaining network.

Several survivability features are inherent to the DDN structure (see Figure 3 on page 14). Features that contribute to DDN's present and ultimate ability to withstand casualties include (1) redundancy, (2) dispersion, (3) dynamic adaptive routing, (4) precedence, (5) graceful degradation, (6) hardening, and (7) reconstitution [Ref. 9: p. 6-1,6-2]. Explanations of each of these terms follow.

1. Redundancy

A second set of equipment provides redundancy for any system. Most of the crucial pieces of DDN equipment have spare parts and redundant capability. DDN

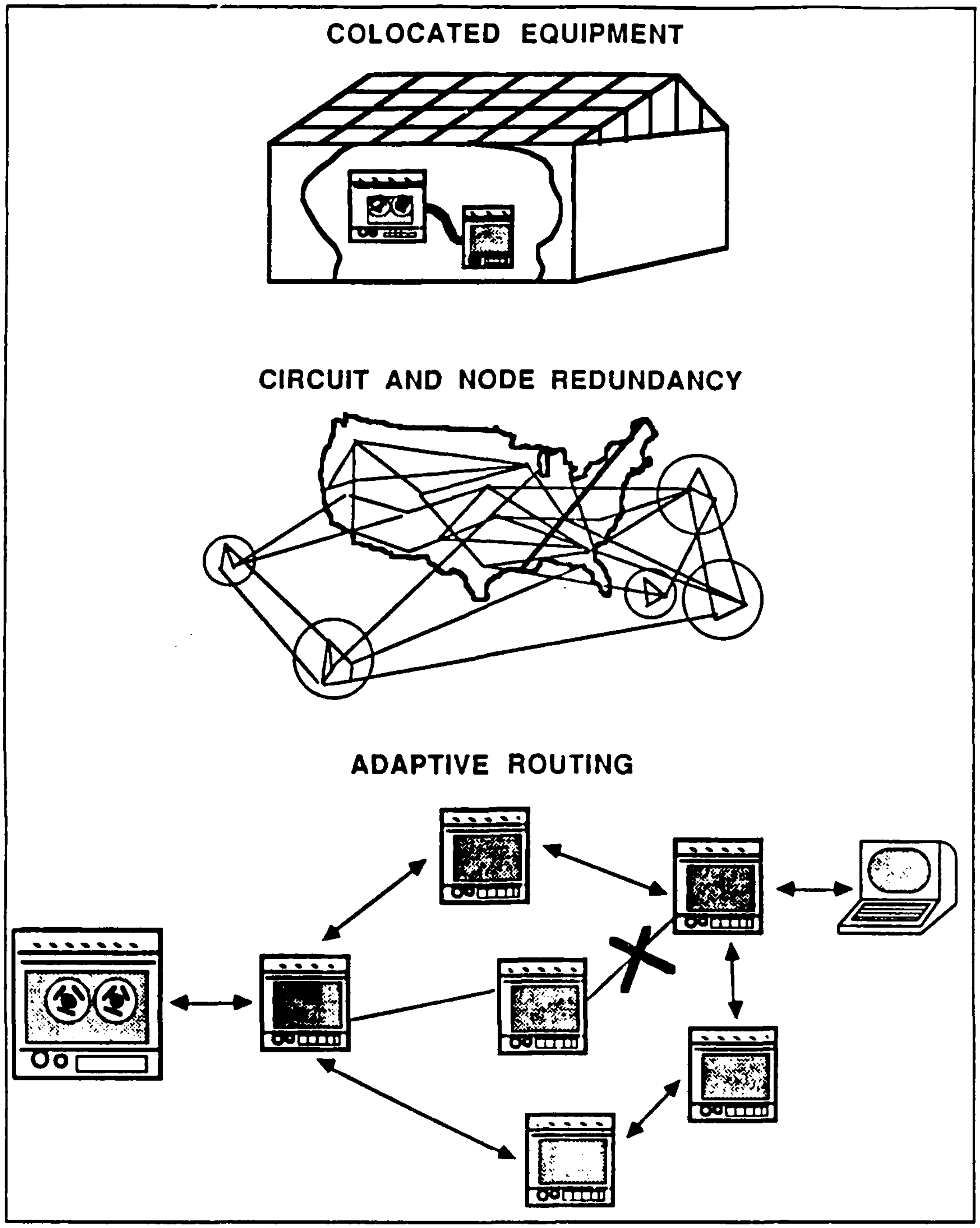

Figure 3. DDN Features Related to Survivability. [Ref. 9: p. 6-1a]

considers packet switching nodes as back-up spares for each other because of their similar operating capabilities. Each of the hundreds of packet switching nodes can process traffic from any source.

The access portion of DDN also has redundant features. Critical users have redundant access lines in addition to back-up computer equipment. This dual homing procedure allows users to reach the DDN through secondary lines, should the primary ones become blocked.

2. Dispersion

The geographical locations of the DDN switching nodes are widely separated. This dispersion enhances survivability because damaged portions of the network can be isolated. The large geographic spread of DDN backbone elements minimizes the damage that any one disaster can inflict.

3. Dynamic Adaptive Routing

Routing routines or algorithms select the path for information to follow through a communications network. Dynamic routing techniques allow two packets going from one source to the same destination to take different paths. Adaptive routing allows a packet to alter paths while in transit. DDN combines these two techniques into dynamic adaptive routing. [Ref. 11: P. 150]

DDN routes each packet individually and updates the chosen route at each switching node. Every node receives continuous updates on the status of all follow-on nodes. The routing algorithms automatically send packets by the most expeditious route. For survivability purposes, this enables packets to avoid damaged nodes.

4. Precedence

DDN packet switching nodes process messages on a first-come, first-serve basis. Preemption mechanisms override this procedure to give priority to important information. Prioritization schemes ensure that critical data go first.

DoD classifies each communication transmission into one of four precedence levels ranging from routine to flash traffic. Mechanisms within DDN ensure that each nodes processes messages according to precedence as well as to time in the system. During peacetime, precedence procedures ensure faster delivery of time-sensitive traffic even if the network is busy. During crises, precedence routines allow users to designate which traffic gets priority on whatever network resources remain intact.

5. Graceful Degradation.

Damage to isolated elements of DDN does not destroy the entire network. If some disaster were to destroy a switching node, the users which normally access DDN through that node would be without communications capabilities (they would probably also be without a lot of other capabilities). Users with access to DDN through other nodes could still have service.

DCA operates centralized regional centers to monitor the status of DDN at all times. These monitors have an overall view of the network and assist with congestion and equipment problems at nodes during peacetime. Should a portion of the network be destroyed, the monitoring centers would probably use the remaining resources to configure a limited network.

6. Hardening.

Structural reinforcement of buildings provides some protection against enemy bombs. Most of the DDN switching nodes are located within a subscriber's facilities. If the subscriber survives to use the node, the switching node should also be operational. The survival of the trunks between nodes is not predictable because of the variations in types (ranging from buried cables to satellite links).

Military planners safeguarding installations in the nuclear age must consider other types of hardening besides strengthening buildings. All DDN components eventually will have electromagnetic shielding and power surge arresting protection against high altitude electromagnetic pulses.

7. Reconstitution.

Prior planning and preparation eases restoration efforts. Even with all of the above-listed survivability features, some segments of DDN could become disabled. After invoking all contingency plans to keep the network operating on a limited basis, DCA will begin restoring DDN to full capability. DCA plans to construct five mobile switching centers to assist network reconstitution efforts. After assessing the situation, DCA will deploy these mobile nodes to provide packet switching during repairs of permanent node sites. The construction of mobile switching centers will increase the flexibility of DDN during peacetime as well as during conflicts.

B. AVAILABILITY

The DDN operates continuously for 24 hours every day. The traffic load may increase during certain hours (daylight working hours for each time zone), but the mission of DDN is to provide communications capabilities for DoD at all times. The

DDN backbone always should be available for access by host computers and user terminals. Three factors that directly affect DDN availability are the reliability of the equipment, the size of the traffic load, and the accuracy of the network.

1. Reliability

The first area of concern for a network user should be his own equipment. DDN subscribers must maintain their own data processing and communication access equipment. Preventive maintenance measures as well as corrective repairs help ensure proper functioning of DDN access equipment. The reliability of the access portion of DDN varies from one subscriber site to another.

If the user's access equipment is working, the backbone should be able to transport data. DCA repairs and replaces equipment for the DDN backbone. When the backbone packet switch nodes are at a subscriber site, DCA assigns a local node site coordinator. The coordinators work with DCA to maintain the packet switches.

Connectors between the switches, the interswitch trunks, also affect the reliability of the backbone. DCA leases most of the interswitch trunk resources from civilian communications companies. The responsibility for the operating conditions of the interswitch trunks belongs to their owners.

The backbone components have performed well to date. DCA has set minimum threshold standards and the operational components of MILNET have met these goals. The minimum acceptable measure of reliability for switching nodes is 98.5%. This level of reliability reflects the percentage of a given period of time that a computer is in good working condition. The average reliability of MILNET packet switching nodes was 99.45% for the first nine months of 1987. [Ref. 12] Figure 4 on page 18 graphically depicts recent node performance on a monthly basis.

The performance of the interswitch trunks has also exceeded management thresholds. DCA demands a certain amount of reliability from its leased circuits but must rely on the lessors to provide it. The minimum acceptable level of trunk reliability is 97%, and the actual level for the first part of 1987 was 98.33% [Ref. 12]. Figure 5 on page 19 shows MILNET interswitch trunk performance for 1986-1987.

The composite system performance of the MILNET backbone is 98.89% reliability. These solid performance statistics are not very reassuring when a user experiences difficulty with the system. To assist users with problems, DCA operates a network monitoring center. Node site coordinators contact the monitoring center for troubleshooting assistance. DCA plans to establish more monitoring centers as DDN

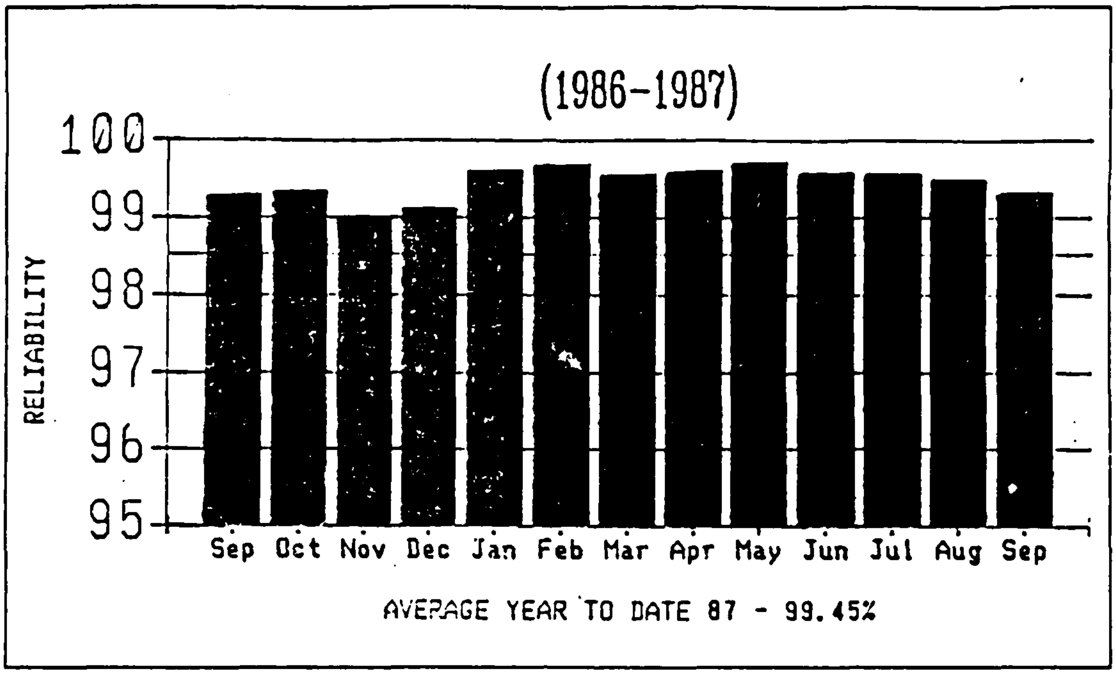

Figure 4. MILNET Packet Switch Node Performance. [Ref. 12]

expands. This centralized coordination helps bring users back on line and disseminates network status information.

2. Delay

Another important measure of the availability of a communications network is the amount of time it takes for a message to reach its destination. Since DDN divides messages into small packets, the delay time for any message depends on that of its slowest packet. The performance of the network depends on its efficiency. Packet switching overcomes inefficient procedures and delivers messages quickly.

High overhead is the primary inefficiency of packet switching procedures. Overhead is any transmission information included in the pa ket that is not part of the message or data flow intelligence. Each packet must contain its destination address, packet sequence, and precedence information. Including these control items with every packet instead of once per message results in duplicate information travelling network resources.

The low message delay times of MILNET prove that disassembling and reassembling messages into packets for transit does not slow information exchanges. The high overhead per message of packet switching is not the most efficient use of

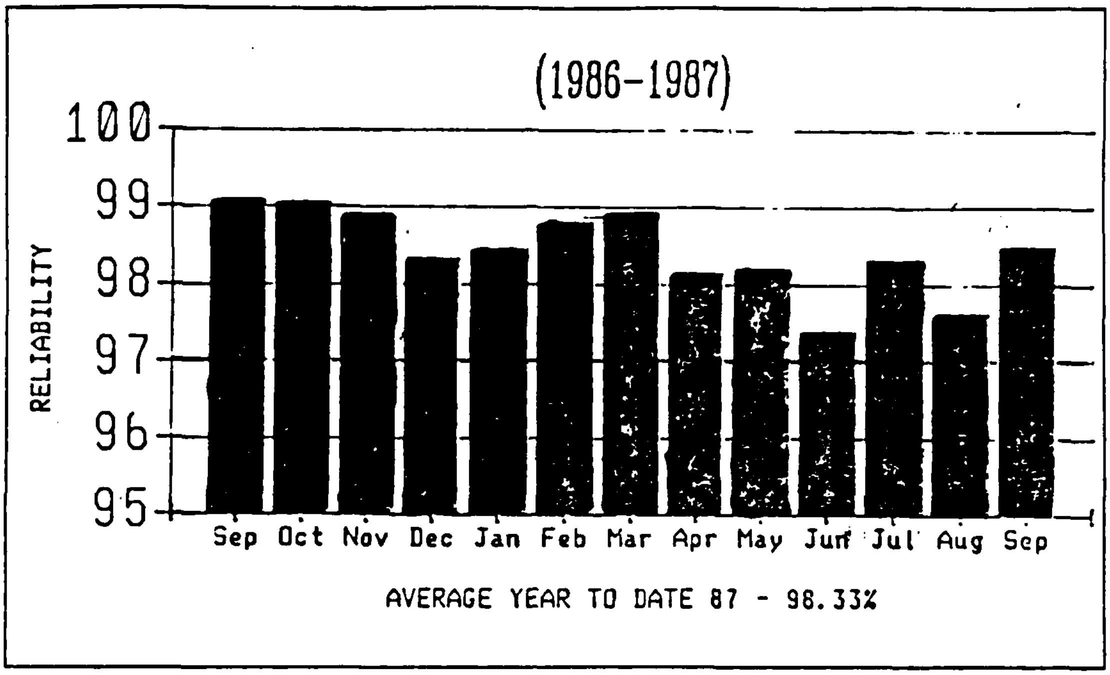

Figure 5. MILNET Interswitch Trunk Performance. [Ref. 12]

packet capacity, and it affects the network transmission speed. The average source-to-destination (end-to-end) time for low precedence MILNET traffic within the continental United States is projected to be less than 200 milliseconds [Ref. 9: p. 6-3a]. This speed would be fast enough for interactive use.

MILNET can often support query and response interactions as well as timely acknowledgements during data transfer. The 200 millisecond delay time averaged over a 24 hour period does not, however, accurately reflect the user's situation. Response time during peak working hours may not be acceptable while the response time in the middle of the night may be almost instantaneous. DCA strives to minimize delays at all times and encourages users to postpone noninteractive, low priority traffic to slack periods. As the number of subscribers continues to increase, DDN resources will have to continue to expand.

3. Accuracy

Reliable, timely communications will benefit no user if errors occur. DDN is available to users and is also extremely accurate. The system employs error detection techniques to ensure error-free transmission through the access devices, access lines, switching nodes, and interswitch trunk circuits. The probability of an undetected error getting through is extremely small, and errors that are detected can be corrected.

As discussed, packet switching divides messages into packets. Each packet consists of a series of bits. Bits are binary digits; they are either zeroes or ones. Computers use languages consisting of only binary digits to process data and to send data to other computers [Ref. 13: p. 300].

The two bit states, zero and one, do not provide much information. Data communications systems group bits together to form binary words. Transmitting words through a communications system may require additional bits for network control or error detection. The term frame refers to a binary word plus any control bits. As the number of bits per word increases, so does the number of different combinations of bits or separate words. Each digital system must use a code (such as the American Standard Code for Information Exchange) to translate binary words into meaningful plain language characters.

A DDN packet can contain up to 1008 bits [Ref. 14: p. 98]. For plain language messages, a bit error may result only in a word misspelling and would probably not affect the message content. For bulk data transfers, a bit error may be more significant and not immediately noticeable. When the system does detect an error, the receiver requests a retransmittal.

DDN uses techniques called 16-bit cyclic redundancy checks to detect errors in the access and trunk circuits [Ref. 9: p. 6-3]. For each binary word, the transmitter attaches a sequence of bits to make the entire frame exactly divisible by a predetermined number. The receiver divides the incoming frame by this same number. If there is no remainder, the receiver does not request a retransmission. The drawbacks of this method are that it does not identify which bit is in error and it adds bits (overhead) to each frame. It is, however, an extremely effective method.

The cyclic redundancy checks identify bit errors that occur during transmission. DDN also has to detect errors during data processing. The subscriber computers use an error detecting code that performs a summation operation on the bits [Ref. 2: p. 563]. These end-to-end accuracy checks are known as 16-bit checksums.

Determining the overall undetected bit error rate for DDN would depend on the accuracy of each user's data processor. Also some errors may never be identified, so meaningful statistics about DDN bit error rates have not been compiled. DCA projects that an undetected error will slip past all the error detection devices only once every 174,000 years [Ref. 9: p. 6-3a].

C. SECURITY

United States government agencies classify information according to its sensitivity. The different levels of classification impose dissemination restrictions on certain information. The restrictions are based on sensitivity level (confidential, secret, and top secret) and on intended recipients (US and Allied governments, DoD, and various departments within DoD). DoD assigns security clearances to all DoD personnel handling classified information. The clearances designate the highest classification level of information that each person can process. Within each level, the information is limited again to only those who require the information for their official duties (need to know).

Mechanical information processors also need security clearances. Identifying the highest level of classified material that a piece of equipment can handle or process, helps limit dissemination. Two areas for security concern related to DDN are communications security and computer security.

1. Communications Security

Communications security involves the protection of information as it is transferred from one location to another. Unauthorized listeners can eavesdrop by gaining direct access to transmission lines (wiretapping) or by collecting signals in the vicinity of transmitters or satellite terminals.

Encryption is the primary method for establishing communications security. To encrypt information means to translate it to another form so that only receivers knowledgeable of the translation code can understand the information. Encryption guards against eavesdropping. Any information overheard will seem garbled to anyone without the decryption key. Metallic shielding of equipment (referred to as Tempest shielding) is the DoD technique that is used to contain signals.

DDN also attains communications security by separating DoD communities that work with information at different classification levels. Each subnetwork uses encryption devices to protect information from the time it is sent until it is received. This compartmentation within DoD limits the chances for disclosures of sensitive information.

Several segments of the DDN support classified data. Blacker front-end computer devices, being installed in 1988, will ensure encryption of data sent from one host computer to another within a community. The Blacker devices between packet switch nodes will enable separate classified networks to use the same backbone nodes and trunk circuits. Guard gateway equipment, scheduled for 1992 development, will eventually allow information to flow from a host in one segment of DDN to a host computer in another segment.

MILNET, the primary focus of DDN for this study, does not support classified data. Yet MILNET must still maintain security measures to prevent unauthorized use. The cumulative effect of collecting unclassified official information traveling MILNET over a period of time could result in sensitive disclosures. DDN has incorporated the following services to safeguard against abuse of network systems.

a. Backbone Link Encryption.

DCA and DDN subscribers are in the process of installing KG-84 cryptographic equipment on all MILNET trunks between packet switching nodes and on all access trunks between host computers and the backbone network. DCA will acquire KG-84s for all hosts that are active before September 30, 1988. After that time, new host subscribers must provide the cryptographic equipment for their end of the host access circuits. These KG devices will encrypt all information that travels the DDN backbone. [Ref. 15]

b. Terminal Link Encryption.

Low cost (approximately S100) encryption and authentication devices are available for users to attach to terminal access lines [Ref. 16]. The placement of these devices, known as LEADs, at user work stations will protect information as it travels to host computers. Figure 6 on page 23 illustrates the use of encryption devices for access links.

2. Computer Security

Computer security measures protect data processors from outside tampering and unauthorized access. Today's data processing environment involves many user terminals and local area networks connecting to one organizational computer. These multiple access points create many opportunities for unauthorized users to gain entry into the system. Physical security measures, such as those discussed in the survivability section of this chapter, provide some protection against outsiders gaining access to terminals. There are, however, dial-in telephone lines that may be used to reach DDN without even being on a military installation.

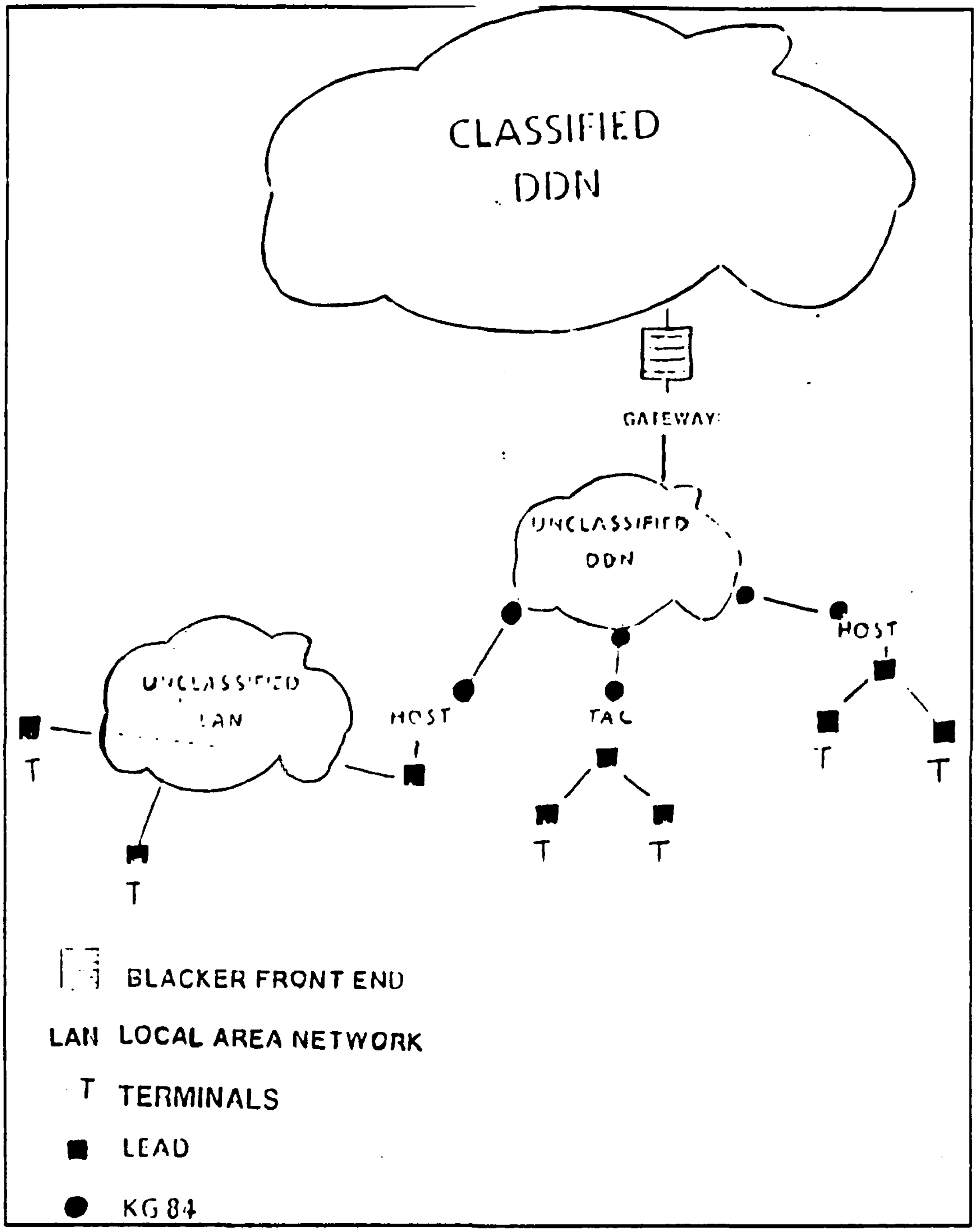

Figure 6. Access Links Encryption Environment.

One solution for computer security in the DDN backbone would be packet switch nodes that could keep information segregated according to classification levels. These trusted nodes are discussed by Lane:

> Today, the network cannot be trusted to properly segregate levels of information so that only the intended recipient reads the transmission. Network switches interconnecting host processors and terminals are themselves processors that cannot be trusted to internally segregate information. The technology exists to build network processors with trusted computing bases, which can be trusted to so segregate, but to date such processors have not been fielded in an operational network environment. [Ref. 17: p. 296]

Packet switch nodes that would separate data from various communities are the ideal.

The actual computer security features of MILNET include user identification and authentication mechanisms. Access control systems require a user to input an identification code (an alphanumeric sequence) and a password. The identification code may be published in order for users to address mail to one another. Passwords are known to authorized users only.

IV. DDN SPECIFICATIONS

This chapter reviews the DDN standards that affect potential subscribers. DCA imposes these standards to ensure that any DDN user can communicate with any other DDN user. DoD organizations that anticipate DDN access should be aware of and consider DDN specifications during the acquisition of any computer or communications systems. The standards are intended to promote interoperability, not to limit flexibility and innovation.

Sections A and B of this chapter describe the hardware and software aspects of DDN. Every command has different needs and resources; these specifications are only general descriptions of DDN options. Section C discusses some of the DDN acquisition requirements and cost factors.

A. HARDWARE

For a computer or communications system, the term hardware refers to physical pieces of equipment. DDN is an excellent example of the merger of computer and communications technologies because its equipment performs many functions. A computer that processes data can also enter that data into the network. Three functions of DDN hardware are data transmission, data processing, and network access.

1. Data Transmission

Long distance information transmission takes place over the DDN backbone. The interswitch trunks are the transmission lines that connect the packet switching nodes. MILNET consists of over 300 leased circuits and satellite backbone links [Ref. 9: p. 5-2]. These links usually process binary information at a rate of 56,000 bits per second [Ref 9: p. 5-4].

The standard DDN packet switching node consists of three types of components, and takes up an area approximately seven feet high, ten feet wide, and three feet deep [Ref. 9: p. 5-11]. One type of component is the cryptographic equipment (KG-84 devices for MILNET). Another node component type consists of the circuit terminating devices. The MILNET terminating devices are called modems (MOdulator-DEModulators), data service units, and channel service units. These devices convert signals to proper format for transmission. The third type of component in the the packet switching node is a Bolt Beranek, and Newman C/30 computer.

The C/30 is an extremely capable communications processor that is programmed to implement the DDN dynamic adaptive routing techniques. Depending on a packet's origin and destination, the C/30 node can serve as a point of entry, a relay station, or a point of exit for the DDN backbone. The Bolt, Beranek, and Newman company has developed an improved C/300 computer that is compatible with the C/30. DCA plans to convert existing nodes to the C/300 as each node reaches its previously scheduled upgrade time [Ref. 18].

As of November 1987, MILNET had 174 operational packet switching nodes [Ref. 19]. Each C/30 node can allow up to 30 host and 14 interswitch trunk connections. To achieve maximum packet throughput rates, the nodes should have no more than eight host and five interswitch trunk connections. The maximum throughput specification for 750-bit packets travelling from one node to another is 175 packets per second. [Ref. 9: pp. 5-14a,5-15]

Each site that houses a DDN node must designate a node site coordinator to interact with DDN program management and the monitoring center. Node Site Coordinator is not a billet programmed into a command's manpower resources so it is usually a collateral duty. During node installation or failure, node coordination can be very time consuming. During routine operation, the time spent on custodial care and administration can be minimal. [Ref. 19]

2. Data Processing

DDN subscribers use many types of computers to store and to manipulate data. These computers range in size from small microprocessors to large mainframes. The user applications of these computers range from word processing to mathematical computation. Each DDN subscriber provides its own information processors, selecting a computer size that meets its particular requirements.

The term host refers to any minicomputer or mainframe computer that uses a packet-switched network to communicate. Every host site assigns a host site administrator. This administrator registers all authorized host users and ensures compliance with network policies and procedures. As local point of contact, the host administrator works with the network monitoring center on host or user network problems. [Ref. 9: p. 11-2]

Terminals are devices that allow direct interface between a user and a computer. The user activates a terminal (usually through a keyboard) to transmit and receive information. Some terminals act only as an interface device between the user and a separate computer. Other terminal work stations are an integral part of a microprocessor (personal computer).

Manufacturers design terminals to work with a particular type of computer. One major difference between terminal types is their synchronization schemes. Transmitters and receivers must coordinate the timing of their communications. This enables the receiver to keep track of the start and duration of each information bit, word, or packet. Asynchronous systems signal the beginning and end of each information character by attaching stop and start bits. Synchronous systems group many information characters together and imbed the timing information in the data signal. Synchronous transmission is a newer method than asynchronous transmission. It is also more efficient because it does not add as much overhead data to the basic message. [Ref. 2: p. 100]

Since DDN was based on older ARPANET technology, it was designed to support asynchronous terminals [Ref. 9: P. 10-1]. Several DDN hardware devices and software implementations have been created to accommodate synchronous transmission and more sophisticated terminals.

3. Network Access

The access portion of the DDN encompasses a variety of computer and terminal connections. Depending on location and communication requirements, a new subscriber may have several alternatives for gaining DDN access. Some subscriber terminals and host computers connect to devices that consolidate several users onto one DDN access line. These devices conserve the limited number of switching node access ports. Options for both host and terminal access methods are described below.

a. Hosts

Figure 7 on page 28 shows three configurations for attaching host computers to DDN. They are (1) the direct method, (2) via a host front end processor, and (3) via a terminal emulation processor.

(1) Direct. Mainframe computers can connect directly to a packet switching node. This type of subscriber does not have to rely on any other access equipment to reach the DDN backbone. It is not, however, a very efficient use of the switching node access port. Another disadvantage of this simple method is that the host computer resources must perform networking functions.

(2) Host Front End Processor. This processor converts all incoming data from the host into formats acceptable for DDN transmissions. It performs the

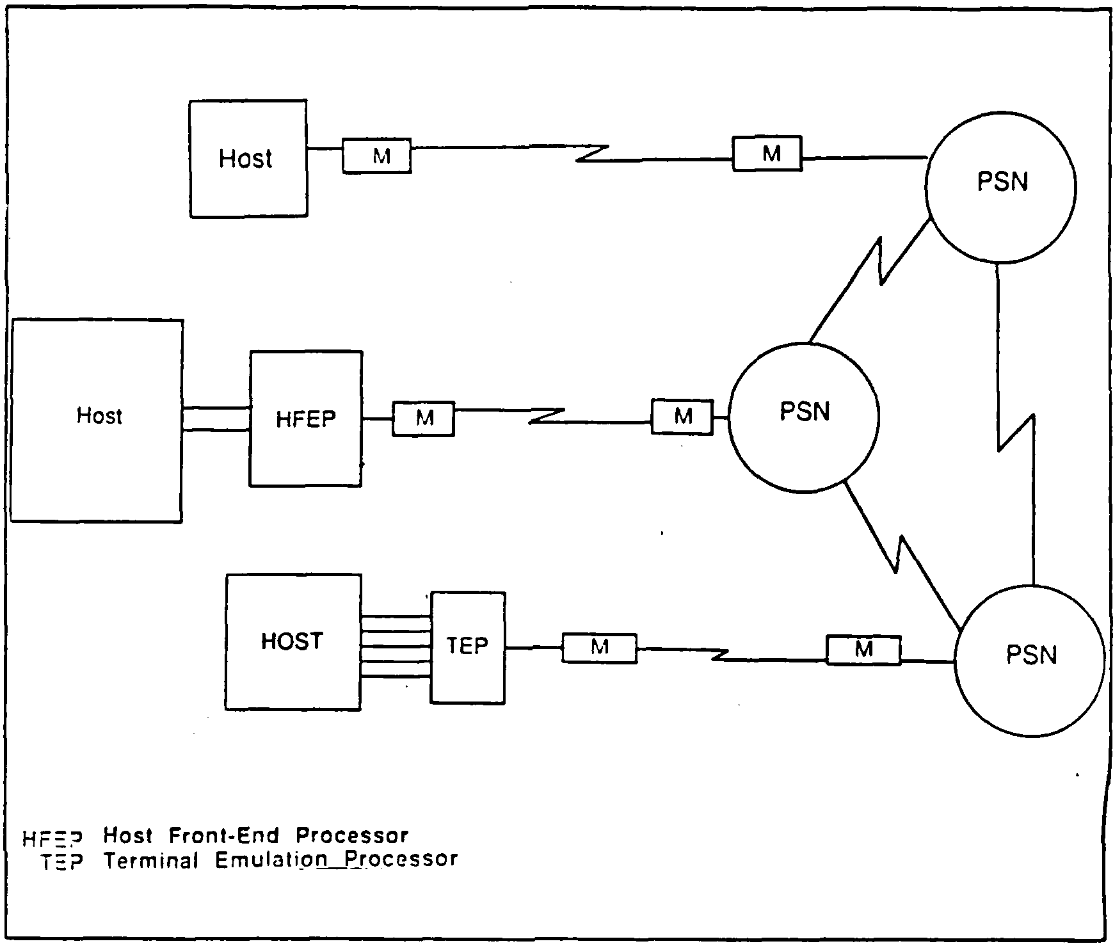
Host
M
M
PSN
Host
HFEP
M
M
PSN
HOST
TEP
M
M
PSN
HFEP Host Front-End Processor
TEP Terminal Emulation Processor

Figure 7. Host Computer DDN Connection Options. [Ref. 9]

networking functions and frees the host computer for data processing. The host front end processor allows two hosts to use one DDN access port.

(3) Terminal Emulation Processor. This component allows terminals to access their remote hosts through the network instead of via a dedicated line to the host. This back door approach allows a host to communicate with terminals but not with other hosts. The terminal front end processor will support up to 16 host terminal ports. [Ref. 9: p. 5-21]

b. Terminals and Personal Computers

Several devices exist that enable terminals to transmit information. Modems convert the data to a format appropriate to the transmission path. Terminals connect to a DDN access component or a host computer by either dedicated circuits or dial-up telephone lines. DCA also offers toll-free (800 number) dial-up access for terminals that can not reach a local network access component or a host computer [Ref. 20].

DCA has deployed a new device that provides an alternative to terrestrial and telephone line transmissions. It is called a Very Small Aperture Terminal and it allows high speed transmissions over long distances. The terminal uses a government satellite to transmit and receive information at a rate of 56,000 bits per second. A total of 12 of these devices were operational in 1987, and DCA projects that 100 will be operational by the end of 1988. [Ref. 21]

DCA also plans to award a contract in 1988 for the delivery of items known as packet assembler/disassemblers. These devices account for differences in terminal types and facilitate communications. The ones developed under the DCA contract will provide DDN interfaces for synchronous terminals. [Ref. 22]

Terminals and personal computers that are not tied in with host computers can access DDN by three methods. Figure 8 on page 30 shows (1) a terminal access controller, (2) a direct connection, and (3) a local area network connection.

(1) Terminal Access Controller. The terminal access controllers are based on the same C/30 communications processors as are the packet switching nodes. Each streamlines access to DDN by consolidating the inputs of 62 asynchronous terminals into one line that connects to the switching node. Terminal access controllers also assist network security efforts by requiring user identification. [Ref. 9: p. 5-17]

Another network access component is the miniature terminal access controller. It differs from the regular controller in that it only has 16 ports and allows synchronous terminal connections [Ref. 9: p. 5-20].

(2) Direct. Only personal computers that can function like host computers can connect directly to a packet switching node. The microprocessor must be able to support the interface software and a dedicated transmission line. This uses up most of the personal computer processing capabilities and limits its usefulness as a host. DCA also discourages this method because dedicating a node access port fulltime to one small computer is not a very efficient use of packet switching node resources. [Ref. 9: p. 10-12]

(3) Local Area Network. DCA has not yet standardized this final method of connecting personal computers to DDN. A local area network configuration would allow local interaction without DDN resources. A gateway device would function

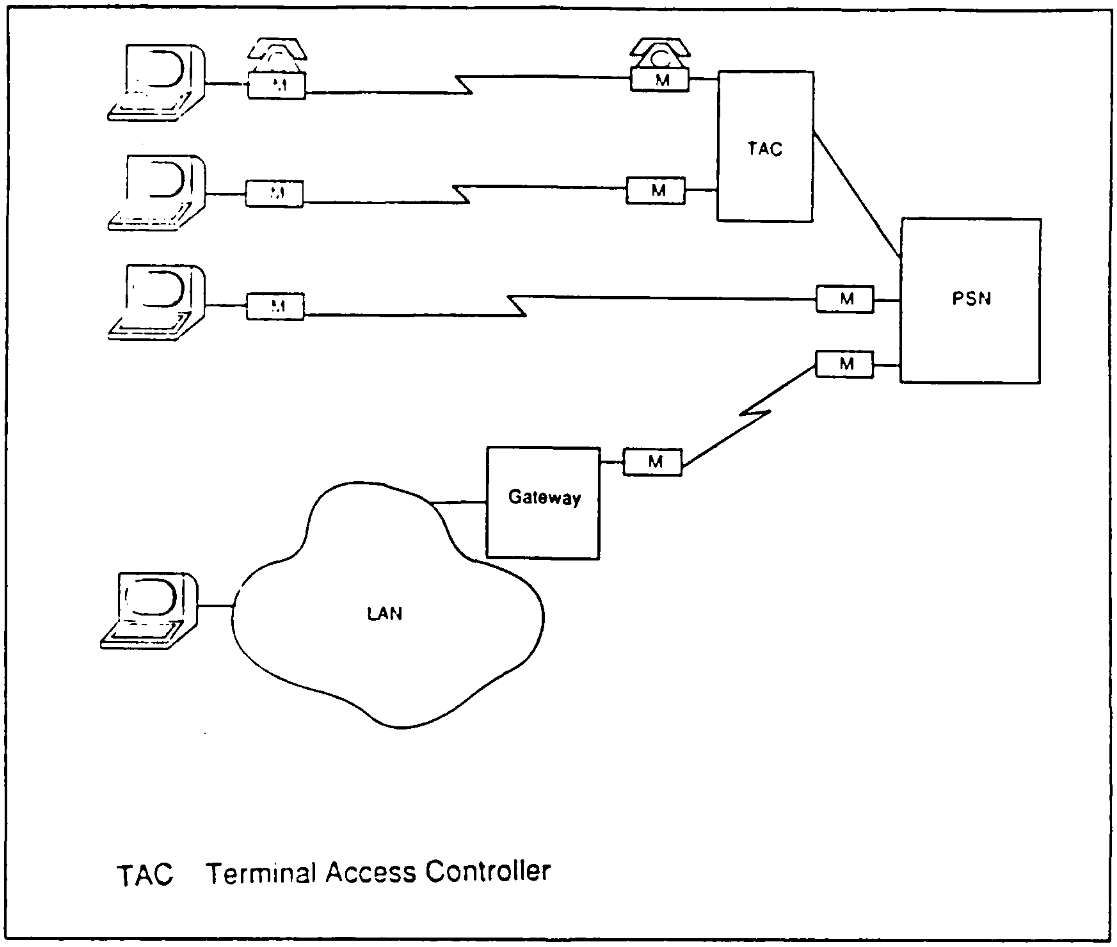

Figure 8. Terminal and Personal Computer DDN Connection Options. [Ref. 9]

like a host front end processor. It would perform the networking functions and free the personal computer processing resources. When gateway devices become standardized, this method will be an efficient use of node access ports. [Ref. 9: p. 10-13]

B. SOFTWARE

Hardware provides the physical connections; software allows communication. Sending information between computers requires a type of language. Computer operators must know the language (or proper sequence of actions at the keyboard) to get the computer to function. Software programs and protocols supply these languages for computer and communications systems.

1. Programs

A program is a sequence of operations to be performed by a computer. A person who knows how to code (write) a program can insert a sequence of operations in the computer memory. An authorized user can then retrieve and run the program any number of times. The number and length of programs stored in a computer depend on its memory capacity. The speed and complexity of program operation depend on both the programmer and the computer capabilities. In addition to accepting input from users who know programming languages, most host computers have useful programs available to all users. The programs on DDN hosts and microprocessors vary from computer to computer. Some examples of types of programs (names will vary) found on many hosts include:

- Directory - lists names of stored files.
- Text Editing - facilitates word processing at the terminal.
- Message - creates and manipulates messages.
- Mail - sends and receives mail.
- Math - performs calculations.
- Statistics - helps prepare spread sheets.
- Record - saves a file of current video terminal display.
- Spell - verifies proper spelling of words in text files.
- Registration - provides current information about network users.

2. Protocols

Protocols are the sets of rules that govern the orderly exchange of information between computers. ARPANET designers originated a set of standard protocols so that participants could use different types and different manufacturer brands of computers (heterogeneous computers). DCA continues to ensure interoperability among DDN subscribers.

Stallings organizes the DoD protocol architecture into four layers. These are called the network access layer, the internet layer, the host-to-host layer, and the process/application layer [Ref. 2: p. 398].

a. Network Access Layer

The protocols in this layer provide for the transfer of data between backbone and access portions of DDN. Packet switching nodes, hosts, and all other network access components must implement these protocols. In addition to allowing data ilow, these protocols perform error detection and message precedence functions. The network access protocols used in DDN are:

- 1822. (This protocol was designed for ARPANET and is not intended for new DDN subscribers.)
- DDN X.25. [Ref. 9: pp. 8-1,8-9]

b. Internet Layer

The protocols of the internet layer permit information to flow from a host on one network to a host on a separate network. The hosts and gateway devices must support these protocols. The protocols for the DDN internet layer are:

- Internet Protocol.
- Internet Message Control Protocol. [Ref. 4: p. 15.5.6]

c. Host-To-Host Layer

The host-to-host layer protocols provide a connection between two hosts that operate on the same network. These protocols facilitate data flow, detect errors, and exchange control messages. The DDN host-to-host protocols are known as:

- Transmission Control Protocol.
- User Datagram Protocol. [Ref. 4: p. 15.5.6]

d. Process/Application Layer

The fourth DoD protocol layer is the process/application layer. It allows computer resource sharing and remote host access. The DDN process/application protocols are listed below and described in chapter V.

- Telnet.
- File Transfer Protocol.
- Simple Mail Transfer Protocol. [Ref. 2: p. 399]

Some readers may be familiar with the International Standards Organization communications model for an open system interconnection. This organization developed its model after the ARPANET standards had been established. The International Standards Organization had the same goal of achieving interoperability among heterogeneous computers. The open systems interconnection model divides the network protocols into seven layers as compared to the four layers of the DoD protocol architecture.

C. ACQUISITION

Current DDN user requirements far outnumber the connection capacity. DCA has begun to develop a system to prioritize all requirements. Two other projects have been initiated to help alleviate the backlog. The Very Small Aperture Terminal program is providing more connection lines. The node upgrades to C/300 computers will provide more access ports to each switching node. Despite these enhancements, projections are that user requirements for host computers will continue to be greater than DDN capacity as shown in Figure 9 on page 34.

Given the current shortage of DDN access ports, it would be unrealistic to detail a timely acquisition plan for DDN host computers for a worldwide organization such as the Naval Security Group. On a priority basis, it would also be unrealistic to assume that nonoperational requirements of the Security Group merit immediate MILNET access. The premise of this thesis is that there presently are host computers and terminal access controllers with available ports. Security Group entities that are located near DoD communications facilities may have easy access to a host computer. Isolated Security Group stations may be able to take advantage of the DDN centralized dial-up (800 number) access.

1. Procedures

Potential subscribers that need host computer or dedicated terminal access must fulfill a number of administrative requirements. The DDN Requirements Implementation Manual contains the procedural information necessary to develop a transition plan. DCA consolidates all DDN access requests in the User Requirements Data Base. This data base supports DCA planning and prioritization. [Ref. 23: pp. 1,2]

Security Group sites will probably not request host connections. They may, however, request access for one terminal. A direct connection between a user terminal and a terminal access controller or miniature terminal access controller must register in the User Requirements Data Base [Ref. 23: p. 7]. The first step is to submit completed versions of DDN-MIS URDB Terminal Questionnaire Form (Form T-1) and DDN-MIS URDB Connection Questionnaire Form (Form C-1) to the Naval Telecommunications Automation Support Center [Ref. 23: p. 6]. Sites that wish to access an existing host need only to coordinate with that host site administrator. The approval of all access requests depends upon the availability of operational access ports.

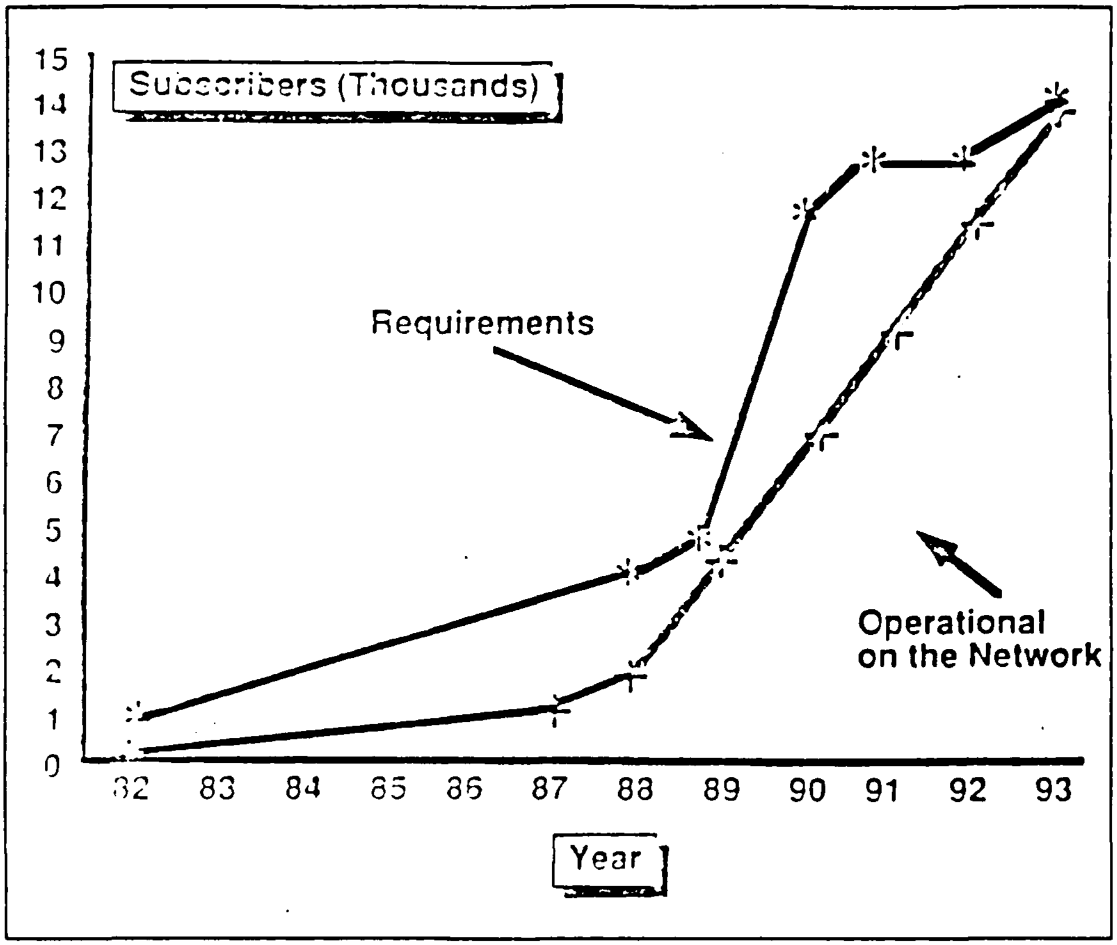

Figure 9. User Requirements versus Operational Hosts. [Ref. 18]

2. Cost

Access to DDN would requires initial implementation costs. A subscriber must provide the terminal, modem, encryption/authenticator device, and packet assembler/disassembler (if required). The price of these items depends on the sophistication of the model purchased.

In addition to implementation costs, communication services have operating fees. At the present time, DCA manages the Communications Services Industrial Fund. This fund recovers the cost of providing DDN services by levying charges on the military departments and any participating DoD agencies. The Commander of the Naval Telecommunications Command supplies the Navy's fixed monthly payment to the centralized fund.

In fiscal year 1990, DCA will charge the DoD agencies and military departments according to actual DDN usage. The Navy plans to bill each major claimant for all user DDN charges. DCA is implementing these usage-sensitive billing methods to distribute costs fairly and to promote network efficiency. The rates will be based on the total number of operational hosts and access line costs. [Ref. 18]

The Commander of the Naval Telecommunications Command will program for all Navy DDN costs for 1990 and 1991. Beginning with the fiscal year 1992 budget, major claimants must submit projected costs based on past DDN usage. Given the present situation of no DDN access, the major claimant COMNAVSECGRU will receive no DDN funds.

3. Training

Any command that acquires a DDN terminal should make training aids available. A list of DDN publications follows.

1. *Navy Planning Guidance for Defense Data Network Implementation*, October 1986.
2. *Navy Requirements Implementation Manual for the Defense Data Network*, November 1987.
3. *Defense Data Network Qualified Host Interfaces*, October 1987.
4. *Exception to DoD Policy on the Use of DDN and Waivers From DoD Policy on Use of Defense Data Network*, November 1987.
5. *Defense Data Network*, undated.
6. *DDN New User Guide*, December 1985.
7. *Network Usage and Cost Sensitivity*, January 1986.
8. *Methods and Procedures - Defense Data Network User Operating Procedures*, April 1987.
9. *Terminal Access Controller User's Guide*, April 1987.
10. *Node Site Coordinator Guide*, September 1986.
11. *DDN Node Planning and Engineering Guide*, September 1986.

Users can obtain these documents from the Naval Telecommunications Automation Support Center [Ref. 23: pp. 1-6]. Video courses are also available from the Support Center and the Bolt, Beranek, and Newman Communications Company. Any individual with a will to experiment can master DDN methods in a short time.

V. DDN ADMINISTRATIVE APPLICATIONS

A. GENERAL APPLICATIONS

The computer and communication merger of the 1970s and 1980s is beginning to impact many organizations. The overlap of the two technologies enables users to send information directly from their work stations. Previously, data processors had to transcribe information into hardcopy message form and deliver it to a central communications center for entry into the long distance system.

The blending of computer and communication technologies into the common field of information systems means enhanced networking capabilities. New computers are more capable and more readily available. New communication systems are faster and more versatile. The users of many types of computers in many locations now share data and information.

The networks of shared resources span long distances. Traditional information transfer methods (such as paper mail, recorded messages, and telephones) are not becoming obsolete. Instead, automatic network functions are increasing the amounts of information that each organization can handle [Ref. 24: p. 76]. Remotely separated associates who formerly exchanged only formal correspondence and reports can now quickly share databases, exchange inquiries, and provide feedback.

Anticipating potential applications for long distance networking requires some imagination. As wide area networking begins to support full interaction between different types of computers, users will probably discover many new capabilities and applications. Oliver expresses this probability in the context of the implementation of an electronic mail network for the civilian company Federal Express:

> People's view about whether to have a telephone once depended upon whether they thought nobody had one or everybody had one. The same with office copy machines and overnight express. Once the habit was accepted, it became an expected way of doing business. [Ref. 25: p. 166]

The transition to DDN will force DoD managers into considering the benefits of a resource sharing network. If changes occur rapidly, the use of network services could become commonplace before the full deployment of internetwork gateway devices. Fully compatible gateway devices have yet to be developed. It is conceivable that a large portion of DoD could be using electronic mail and transferring data files over MILNET while those organizations still using AUTODIN or another network would be unable to participate.

The Naval Security Group does not plan to access MILNET or any of the classified segments of DDN directly. A worst case (but possible) scenario of the future is one where NSGAs are among the few Navy entities that do not have DDN addresses in a DoD directory. The NSGAs could still send and receive official messages but could not take advantage of electronic notes, DoD electronic bulletin boards, and other valuable information services. This scenario is not too far-fetched when one considers that the Standard Navy Distribution List is scheduled to be available for public access on DDN in 1988 [Ref. 26]. It will contain the electronic mail addresses of those commands that accept electronic mail.

This chapter suggests possible administrative DDN applications for the Security Group. Ideally, all of a command's divisions and departments would be connected to an unclassified local area network that would have a single line to the nearest DDN host or node. More realistically, these proposed applications are based on the assumption that each Security Group entity could obtain at least one DDN-compatible microcomputer. There are not enough applications to justify the purchase of a host computer. Instead, the access to DDN could be through a base host computer or directly to the nearest terminal access controller. The terminal should be located in a centralized place away from the processing of any classified material. Some commands might place the DDN terminal in the Career Counselor's office or on the Quarterdeck. Other commands might choose the Administration Department spaces.

1. Administration

Every Naval Security Group entity needs administrative support. The centralized administration department or division monitors the correspondence and record keeping of a command. Every letter to be signed by the commanding officer must first pass through Administration. The personnel assigned to Administration already operate a variety of word processing and automatic data processing equipment. They would need only a minimal amount of training to operate DDN-compatible terminals.

Administrative cryptologic technicians work in the operations, communications, and electronic maintenance functional areas. They prepare letters and messages and maintain appropriate filing systems. An ideal goal of NSGA's is to have all administrative personnel connected on a local network.

The Security Group does not have base local area networks yet. There are, however, many ways the Administration departments could benefit from MILNET. The first way that MILNET could help would be by eliminating some formal correspondence. The following paragraph from the "Correspondence Management" chapter of the *Navy Correspondence Manual* indicates that alternatives to formal letters are desirable:

> Preparing correspondence is time consuming and expensive. Don't write unless you must. A conversation in person or by phone often saves two letters, the one you would have written and the one the other person would have answered with. Conversations are often better than correspondence for working out details that require give and take. You can always confirm a conversation by a memo to the other person or a memo for your records. [Ref. 27: p. 10-1]

The networking functions of MILNET offer an informal way to communicate without going through the timely process of routing a typewritten letter through the chain of command for release. Follow-up memos would not be necessary because users can record and store electronic conversations taking place over MILNET.

In addition to correspondence functions, NSGA Administration Departments supervise the command's performance with regard to periodic reports. The reports range from manpower allowance figures to Inspector General Inspection follow-ups. The cognizant departments submit reports to the Administration Department for the Commanding Officer's signature. A wide area network like MILNET could facilitate COMNAVSECGRU's call for these reports. Each command could store recurring reports on the microcomputer and then easily update and amend them for submission.

2. Personnel

A separate activity or detachment performs most of the personnel support functions for the Naval Security Group. Even though NSGAs do not handle most of the official service and pay record functions, they do have an obligation to ensure that all personnel are receiving proper service and fair entitlements. As the Navy Finance Center and Personnel Support Activities and Detachments transfer to DDN, accurate and timely information about personnel matters will be available. Two payroll and financial systems scheduled for DDN access in the near future are the Joint Universal Pay System and the Automated Budget Interactive Data Environment System [Ref. 28: p. 6]. Access to MILNET would enable Naval Security Group managers to be informed liaisons between their sailors and personnel support groups.

Another area with planned DDN applications is the military health services. The Triservices Medical Information System and the Defense Eligibility Enrollment System are both slated for DDN access [Ref. 28: pp. 5-6]. NSGAs that provide medical and dental services should be aware of the availability of medical record keeping systems.

3. Supply

The Navy Supply System is already converting to DDN. The Navy Stockpoint Logistics Integrated Communications Environment is one of the first sets of networks to begin its transition to DDN. It is a system of local area networks that support the automatic data processing functions of Navy stock points and inventory control points. Two Stockpoint Logistic host computers are operationally attached to DDN packet switch nodes, and 22 more are scheduled to become operational [Ref. 12].

The amount of supply and logistics staffing needed for NSGAs varies from site to site. A command that is a tenant on a base may only need a few storekeepers within the electronic maintenance department to handle the operational equipment inventories. A self-sufficient, isolated command needs a full department of Navy Supply Corps personnel. Coordinating a timely connection to MILNET with the Supply Corps may prevent these departments at NSGAs from becoming isolated from their parent communities.

4. Public Works

Some NSGAs have Public Works departments that either directly maintain base facilities or work through contractors to maintain them. These construction and engineering personnel plan and coordinate most of their projects over unclassified DoD communication circuits. If the Navy Civil Engineering community shifts to DDN, NSGA Public Works personnel may miss out on opportunities to network with both their military bosses and civilian project points of contact.

5. Staff Elements.

Security Group personnel serve on shore-based staffs of Fleet Commanders in Chief as well as that of COMNAVSECGRU. Allowing these individuals access to MILNET may facilitate better coordination with their counterparts. As DDN usage grows, Security Group personnel filling staff billets may find themselves the last to find out about other staff elements' positions on topics that are informally discussed over DDN. If Navy organizations begin to rely heavily on MILNET, it may become difficult for the District of Columbia COMNAVSECGRU Headquarters staff to coordinate with other Washington agencies such as Naval Telecommunications Command or Space and

Naval Warfare Systems Command. A hypothetical example is: if someone sends out a DDN electronic mail note to all concerned parties about a meeting, they may not remember or care to notify the cryptologic element by other means.

6. Collateral Duties

Many of the time-consuming collateral duties performed separately at each NSGA could be streamlined through networking. The physical fitness coordinator at one site could share with others the most efficient statistical spread sheet to use for tabulating physical readiness test data. A Command Automatic Data Processing Security Officer could compare his station instruction with those of other sites. Combined Federal Campaign and Navy Relief fund raisers could coordinate with other organizers. In many instances, morale probably would be improved by any offers of assistance and the knowledge that others are performing the same collateral duties.

B. DIRECT APPLICATIONS

1. Electronic Mail

In the broadest sense, electronic mail is defined as a system of electrical devices that send messages. This definition could include the telex and facsimile message systems that are used by many civilian communities. Telex consists of teletypewriter telegraphs connected to telephone lines. Facsimile machines scan printed, graphic, or handwritten pages and then electronically transmit the contents over telephone lines [Ref. 29: p. 133].

In the context of DDN and most other computer networks, electronic mail is a network function that allows the exchange of messages from one computer terminal to another. However, electronic mail notes, memos, letters, and data are not presently considered to be standard Navy messages. They differ from telex, facsimile, and traditional Navy messages in several ways. The primary difference is that electronic mail routes information directly from the sender's terminal keyboard to the receiver's terminal display. Traditional methods require message originators to print the information at a device that is physically separate from the communications system.

Another way that electronic mail differs from standard Navy messages is accountability. Electronic mail does not segregate messages according to classification and precedence levels. AUTODIN and DDN assign DoD messages an identification number consisting of the date and time of origination and all messages are retained for a certain number of days. The DDN electronic mail system is not standardized. Some host computers only keep track of electronic mail messages that are sent, and others indicate to the originator the time of receipt of a message at the destination terminal.

Electronic mail is a fairly new concept in networking for DoD. Organizations are still experimenting with procedures and applications for electronic mail. The Naval Data Automation Center is the largest Navy organization now using DDN on an operational basis. They have used electronic mail for internal project management and for financial transactions with field stations (Naval Regional Data Automation Centers). Based on their experience and a Joint Chiefs of Staff policy memorandum concerning electronic mail, the Data Automation Command has established some electronic mail guidelines that may benefit other organizations. The guidelines emphasize that this mail system is not a service of DCA but is instead procured and funded by the users. [Ref. 26]

The Naval Data Automation Command based their electronic mail policy on a traditional mail room concept. Postal service letters can be either formal or informal depending on who signs them, whether they are on official letterhead paper, and whether they were serialized by the mail room. Similarly, electronic mail can be routed through a mail room type of terminal for each command. Serialization by the mail room will identify an item as official. [Ref. 26] This type of centralized control mechanism could be adapted to an NSGA administrative DDN terminal. An accountability log would deter frivolous use of the system.

The DDN electronic mail service does allow users to send messages directly to other users' terminals. The specific capabilities of the mail handling programs vary from one host computer to another. Most of the mail programs feature the following commands:

- Send. Users can initiate, forward, or respond to messages from their terminals.
- Read. Message headers may be viewed first and then individual messages may be displayed.
- Print. The print capability depends on the availability of a printer for the user's terminal.
- Move. Recipients can store incoming messages in files or delete them. [Ref. 5: pp. 25-26]

a. Advantages

Subscribers can use electronic mail as a substitute for the telephone. When interactive dialogue is not necessary, a message sent electronically can provide information or ask questions. Recipients can research their responses and answer at their convenience. This system circumvents the telephone tag games of callers trying to find their points of contact at their desk and free to answer. Within DoD, electronic mail alleviates struggles to find a free AUTOVON line and solves the problems associated with large time zone differences. Electronic transfer of notes also allows precedence systems of the network and prioritization by the recipient to take place without affecting the initiator.

In many instances, electronic mail can replace postal, speedletter, or formal message services. Electronic mail facilitates networking at interorganizational levels lower than that of commanding officers.

b. Disadvantages

The major drawback of electronic mail is the negative reaction by DoD organizations reluctant to change. Many that have implemented electronic mail have used it only on an informal basis similar to the use of telephones. However, unlike the telephone, electronic mail provides a written record of correspondence which may later be used for accountability purposes. Commanding officers will have to establish internal and external command policies governing the official status of electronic mail. As electronic mail becomes more accepted, DoD organizations will have to meet the challenges of security, authentication of sender, and guarantee of delivery [Ref. 17: p. 294].

c. Security Group

The Department of the Navy Correspondence Manual allows for electronic mail as a promising method of communications [Ref. 27: p. 10-4]. Potential applications for Security Group elements include:

(1) Career Counseling. Sailors could easily update preference cards. Detailers could submit latest assignment possibilities. Neither party would be put on the spot to respond without time for some consideration.

(2) Legal. The answers to legal questions must often be researched. Legal officers in remote sites such as NSGA Adak, Alaska, could tap into the expertise of the COMNAVSECGRU headquarters legal staff.

(3) Sponsors. Streamlining the flow of information between sponsors and people changing duty assignments may ease the transfer process. Last minute schedule changes could be shared rapidly and conveniently.

(4) Travel. Questions regarding temporary additional duty assignments could be directed to the appropriate point of contact. Travel arrangers could exchange the latest lodging and accounting information.

2. Telnet

The telnet function of DDN permits a user working at one host to operate as if he were signed on to another host computer. This remote log in capability enables the user to access databases, run programs, and perform other operations as if the resources were on his own computer [Ref. 5: p. 34].

The telnet function is easy to use. The *DDN New User's Guide* lists the following steps for running telnet:

- Log in to an initial host.
- Invoke the telnet program on that host.
- Identify by hostname or host address the remote host you wish to access.
- Once connected to the remote host, log in with user name and password for that host.
- When finished working on the remote host, type the command to log out. Then break the connection. You are now back where you began on the initial host. [Ref. 5: p. 35]

a. Advantages

Large data bases can be centrally maintained and updated. Information resources can be shared by all authorized subscribers. Telnet allows remote users to run programs within their intended computer environments. It also spares users of large data bases or long programs from having to obtain adequate local storage capacity.

b. Disadvantages

Data base managers must implement protective measures to prevent tampering. Resource centers which allow users to add or change information in addition to reading files must authenticate the identity of the users and verify the input.

c. Security Group

(1) Bulletin Boards. Electronic bulletin boards are an easy way to disseminate information to network users. These centrally maintained newsletters or data tables can be valuable resources. Telnet allows users from any host to access DDN bulletin boards.

(2) Maintenance. The new Security Group electronic maintenance equipment requirements system involves the transfer of inventory lists recorded on

floppy disks. Implementation of DDN's telnet function would be more efficient than mailing diskettes all over the world.

(3) Communications Security Material System. The Director of the Communications Security Material System has begun to automate the distribution of cryptographic keying material. As the system evolves to one of bar-coded inventory procedures, Security Group sites could accomplish the unclassified bookkeeping over MILNET.

3. File Transfer Protocol

The file transfer protocol capability allows for the transmission of an entire file from one computer to another. Since files can contain data, programs, or text, this function has a variety of applications.

To access a remote host, a user must identify that host name and address. A valid user name and password for the remote host are required. Users can protect their files by identification codes. Only authorized files can be received and sent during the file transfer process. The *DDN New User's Guide* general steps for transferring a file are:

- Log in to the local host, and invoke the file transfer protocol program.
- Provide the host name or host address for the remote host.
- Once connected to the remote host, log in with user name and password.
- Issue commands to copy or send files.
- When finished, log out from the remote host, and exit from the file transfer protocol program. [Ref. 5: p. 32]

a. Advantages

Data base managers can use the file transfer protocol to send entire files of data within their original file structure. This would allow the receiver to manipulate the data with the same statistical spread sheet functions. The expertise and power of a computer program stored in a file can be shared immediately. Text files can be drafted, sent, revised, and returned any number of times with the file transfer protocol.

b. Disadvantages

Transferring text files to be edited does not preserve the original or denote the author of individual changes. File transfers can be lengthy so the procedure must be conducted at low priority in the network.

c. *Security Group*

Security Group personnel could benefit by sharing programs they have developed. In addition, the DDN Network Information Center provides user assistance and computer operations references to all subscribers.

(1) Text Files. Documents sent to NAVSECGRU headquarters for submission to other authorities such as awards boards could be transferred as a files to allow for easy revisions.

(2) Command History. Submission of the annual command historical reviews by electronic means would facilitate easy paperfree storage in a central data bank at COMNAVSECGRU headquarters.

VI. CONCLUSIONS AND RECOMMENDATIONS

The technical information presented in this thesis demonstrates that DoD communication methods are becoming decentralized. On a broad scale, the AUTODIN switching centers will be replaced by hundreds of DDN packet switching nodes. On a smaller scale, DDN now distributes to the numerous user input terminals many communication functions that were previously handled by communications centers.

One can only guess at the extent to which DDN will become an interoperable wide area network for DoD. The office automation functions that local area network operators now enjoy could become standard for all of DDN. Naval Security Group entities may not be able to participate in this communications revolution if networking over DDN becomes common before NSGAs develop the capacity to use internetwork gateways and interservice/agency message processing.

A. CONCLUSIONS

The following conclusions can be drawn, based on the information reviewed for this study.

- MILNET is operational and performing well for a limited number of users.
- Packet-switched networks offer valuable networking resources that no other DoD telecommunications system offers.
- Electronic mail is a promising communications tool that has not gained complete acceptance by DoD, but that appears to be growing in popularity.
- DDN billing methods are in a period of transition.
- DDN acquisition procedures require advance planning.
- The Naval Security Group is not presently planning to access the DDN directly.
- If the Naval Security Group were to support direct-access DDN services, the following benefits could be realized:
  1. Improved networking capabilities between Naval Security Group sites and other DoD commmands.
  2. Increased sharing of resources and ideas among Security Group personnel.
  3. Expanded administrative communications capabilities for exasperated AUTOVON users and for Security Group personnel isolated by time zones.

B. RECOMMENDATIONS

The findings and analysis of this thesis result in the following recommendations.

- Naval Security Group personnel who are involved with the transition of DoD cryptologic communities to a separate packet-switched network should study the DDN lessons learned, and apply them wherever possible during network development.
- NSGA department heads and communications managers should become familiar with MILNET and with the communications procedures of staff communities such as Supply Corps and Civil Engineer Corps.
- Each command located near an available DDN host or terminal access controller should investigate the feasibility of connecting at least one terminal to that host, so that existing DDN communications capabilities can be used as soon as possible for Security Group functions.

LIST OF REFERENCES

1. Stoner, J.F., *Management*, 3rd ed., Prentice-Hall, Inc., 1986.

2. Stallings, W., *Data and Computer Communications*, Macmillan Publishing Co., 1985.

3. Chernikoff, L. and Pollen, L., *Applications of Integrated Service Digital Networks in the Defense Communications System*, Proceedings of EASCON, IEEE, 1985.

4. Tice, R.M., *Connecting to the Defense Data Network using the DCA's Network Access Component*, Conference Record of IEEE Military Communications Conference, October 1986.

5. Dennet, S.C., ed., *DDN New User Guide*, Defense Communication Agency, DDN Network Information Center, December 1985.

6. Boutacoff, D.A., "DDN Evolves To Meet Interoperability, Security Needs," *Defense Electronics*, April 1986.

7. Hurlbut, J.H., "An Approach To Integrating Defense Data Communications," *Government Executive*, June 1984.

8. Deputy Secretary of Defense Memorandum to Secretaries of the Military Departments, Subject: *Defense Data Network (DDN) Implementation*, March 10, 1983.

9. *The DDN Course*, Network Strategies, Inc., April 1986.

10. Baxter, A.G., COMNAVSECGRU Headquarters Staff, Washington, D.C., personal communication, November 1987.

11. Fidelman, M.R., and others, "Survivability Of The Defense Data Network," *SIGNAL*, May 1986.

12. Damon, T., *DDN Operations*, Navy DDN Program Management Review, November 1987.

13. Stanley, W.D., *Electronic Communications Systems*, Prentice-Hall Co., 1982.

14. BBN Communications Corporation Report 6098, *Network Usage and Cost Sensitivity*, by J. Kane and others, January 1986.

15. Mundy, R., *Defense Data Network Security Architecture: An Overview*, Navy DDN Program Management Review, November 1987.

16. Wise, M., *Low-cost Encryption/Authentication Device Status*, Navy DDN Program Management Review, November 1987.

17. Lane, J.J., "Challenges in Communications for Command and Control Systems," *Digital Communications*, Thomas C. Bartee, ed., Macmillan Inc., 1986.

18. Schreiner, D., *DDN Overview*, Navy DDN Program Management Review, November 1987.

19. Somers, P., *Navy Node Status*, Navy DDN Program Managemant Review, November 1987.

20. Leonard, R., *800 Service For Terminal Users*, Navy DDN Program Management Review, November 1987.

21. Leonard, R., *Very Small Aperture Terminal*, Navy DDN Program Management Review, November 1987.

22. Rauen, K., *Synchronous Terminal Connections*, Navy DDN Program Management Review, November 1987.

23. Naval Telecommunications Automation Support Center, *Navy Requirements Implementation Manual for the Defense Data Network*, Draft report, November 1987.

24. "Electronic Mail: User Boom," *Data Communications*, April 1986.

25. Merwin, J., "Anticipating the evolution," *Forbes*, November 4, 1985.

26. Norem, D., *E-Mail Policy*, Navy DDN Program Management Review, November 1987.

27. Secretary of the Navy, *SECNAVINST 5216.5C - Correspondence Manual*, August 24, 1983.

28. BBN Communications Corporation Report 6096, *Type of Service Routing Requirements - Interim Report*, by M. Gardner, November 1985.

29. O'Reilly, J.J., *Telecommunications Principles*, Van Nostrand Reinhold (UK) Co. Ltd, 1984.

INITIAL DISTRIBUTION LIST

		No. Copies
1.	Defense Technical Information Center Cameron Station Alexandria, VA 22304-6145	2
2.	Library, Code 0142 Naval Postgraduate School Monterey, CA 93943-5002	2
3.	Prof. Judy H. Lind Naval Postgraduate School Code 55Li Operations Research Department Montery, CA 93943-5000	2
4.	Mr. Eugene Baxter Comnander Naval Security Group Code G30 3801 Nebraska Avenue, N.W. Washington, DC 20390	2
5.	Lt Bryan Bartsch Commander Naval Security Group Code G333 3801 Nebraska Avenue, N.W. Washington, DC 20390	2
6.	Lt Tracy Hennings Commander Naval Security Group Code G30 3801 Nebraska Avenue, N.W. Washington, DC 20390	1
5.	Lt Jean Eberhardt Commanding Officer Naval Security Group Activity Fort George G. Meade, MD 20755-5290	4
6.	Prof. D.C. Boger Code 54Bo Naval Postgraduate School Monterey, CA 93943-5000	1